

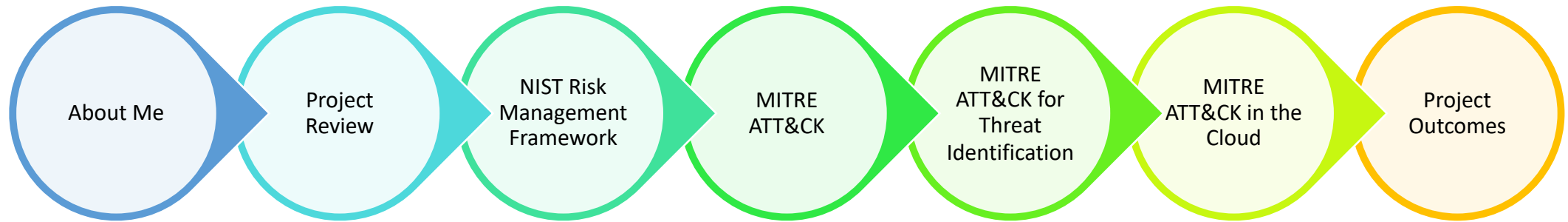
# Improving NIH Cybersecurity Using MITRE ATT&CK

Jared Stancombe

Civic Digital Fellow, Coding It Forward

National Institutes of Health

# Presentation Agenda



# About Me

## Cybersecurity Experience

- M.S. Cybersecurity Risk Management from Indiana University
- Former Incident Response Analyst, Indiana University
- Research with the NATO Cooperative Cyber Defence Centre of Excellence
- 2019 & 2020 Semifinalist, Atlantic Council Cyber 9/12 Strategy Challenge

## Social Impact Work

- Global Health Corps Fellow, Action Africa Help International, Zambia
- William J. Clinton Fellow, American India Foundation
- AmeriCorps Member, City Year Washington, DC
- Board Member, United Way of South Central Indiana

## Previous Government Experience

- Management and Program Analyst, DHS USCIS
- Program Officer, USAID DELIVER Project



# Projects



Conduct research on how to apply MITRE ATT&CK in the NIST Risk Management Framework assessment and authorization process.



Write a wiki article on using MITRE ATT&CK for cloud service platforms.



Conduct a “Lunch and Learn” presentation with relevant NIH stakeholders on using MITRE ATT&CK to identify threats in Security Assessment Reports (SAR).

# Why are these projects important?



MITRE ATT&CK is becoming the language of threat management within the cybersecurity community and NIH does not currently use it.



Current means of threat identification is a “paperwork exercise” and not based upon identifying areas of real risk, but instead used to check a box.



Identifying actual threats can inform how to better identify, detect, and mitigate against them.



NIH InfoSec is heavily siloed. MITRE ATT&CK can encourage inter-team collaboration to improve NIH cybersecurity maturity and efficacy.

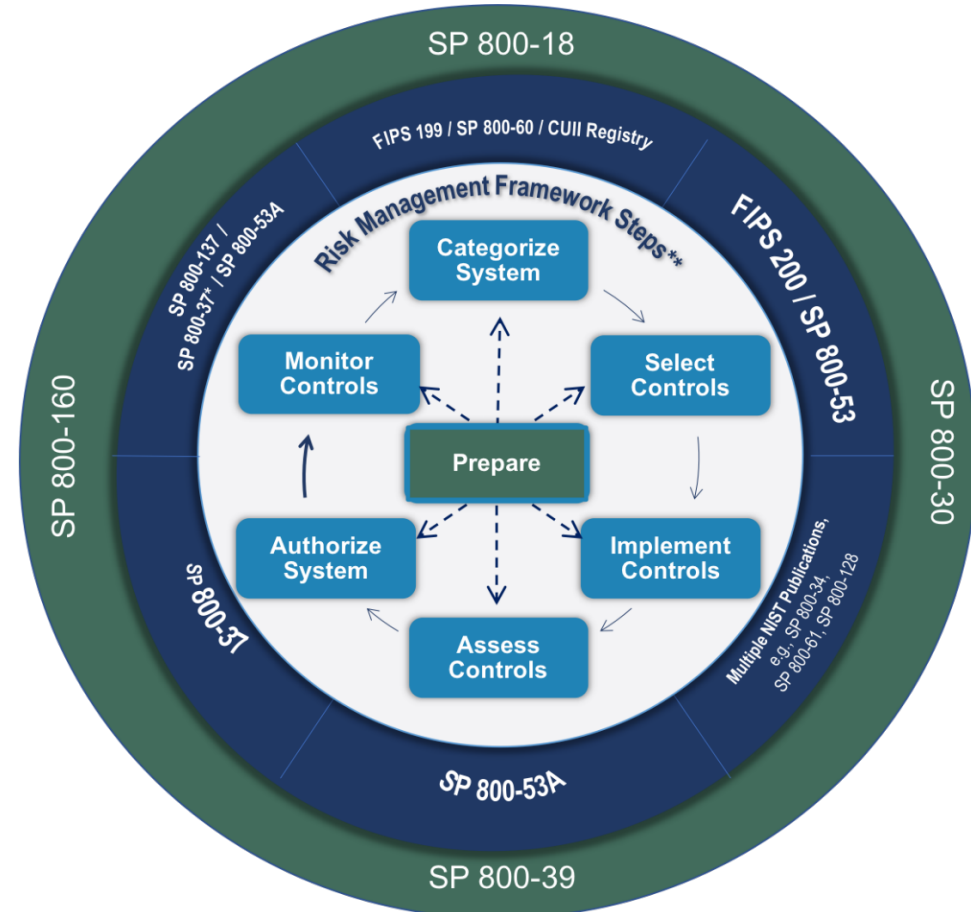
# NIST RMF: Assessment & Authorization

## Assess Controls

- Determines if the controls selected for implementation are:
  - implemented correctly
  - operating as intended
  - producing the ***desired outcome*** with respect to meeting the ***security and privacy requirements*** for the system and the organization

## Authorize System

- Determine if the security and privacy risk (including supply chain risk) to organizational operations and assets, individuals, other organizations, or the Nation based on the operation of a system or the use of common controls, is acceptable.



# Threat Identification in Security Assessment Reports

- **Generic identification** of physical, environmental, & man-made threats
- **Generic categorization** of purposeful, unintentional, or environmental threat categories
- **Generic assessment** of threats & risks based upon potential impacts:
  - Modification of data
  - Data destruction
  - Unavailable accurate records
  - Denial of service
- **Compliance-oriented**

ID	Threat Name	Type Identifier	Description	Confidentiality	Integrity	Availability
T-1	Alteration	U, P, E	Alteration of data, files, or records.		Modification	
T-2	Audit Compromise	P	An unauthorized user gains access to the audit trail and could cause audit records to be deleted or modified, or prevents future audit records from being recorded, thus masking a security relevant event.		Modification or Destruction	Unavailable Accurate Records
T-3	Bomb	P	An intentional explosion.		Modification or Destruction	Denial of Service
T-4	Communications Failure	U, E	Cut of fiber optic lines, trees falling on telephone lines.			Denial of Service
T-5	Compromising Emanations	P	Eavesdropping can occur via electronic media directed against large scale electronic facilities that do not process classified National Security Information.	Disclosure		
T-6	Cyber Brute Force	P	Unauthorized user could gain access to the information systems by random or systematic guessing of passwords, possibly supported by password cracking utilities.	Disclosure	Modification or Destruction	Denial of Service
T-7	Data Disclosure Attack	P	An attacker uses techniques that could result in the disclosure of sensitive information by exploiting weaknesses in the design or configuration.	Disclosure		
T-8	Data Entry Error	U	Human inattention, lack of knowledge, and failure to cross-check system activities could contribute to errors becoming integrated and ingrained in automated systems.		Modification	



How can we improve the  
identification of threats  
to NIH systems?



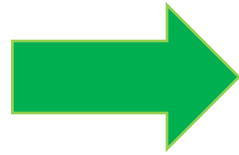
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 techniques	10 techniques	18 techniques	12 techniques	34 techniques	14 techniques	24 techniques	9 techniques	16 techniques	16 techniques	9 techniques	13 techniques
Drive-by Compromise	Command and Scripting Interpreter (7)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application		Exploitation for Client Execution		BITS Jobs	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	Access Token Manipulation (5)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Hardware Additions		Native API	Boot or Logon Autostart Execution (11)		Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking (2)			Clipboard Data
Phishing (3)	Scheduled Task/Job (5)	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Direct Volume Access	Input Capture (4)	Domain Trust Discovery	Remote Services (6)	Data from Cloud Storage Object	Data Obfuscation (3)	Exfiltration Over C2 Channel	Defacement (2)
					Man-in-the-Middle (1)	File and Directory Discovery		Replication Through Removable Media	Dynamic Resolution (3)	Disk Wipe (2)	
Spearphishing Attachment	Shared Modules	Browser Extensions	Create or Modify System Process (4)	Execution Guardrails (1)	Modify Authentication Process (3)	Network Service Scanning	Software Deployment Tools	Data from Information Repositories (2)	Encrypted Channel (2)	Exfiltration Over Other Network Medium (1)	Endpoint Denial of Service (4)
Spearphishing Link	Software Deployment Tools	Compromise Client Software Binary		Exploitation for Defense Evasion	Network Share Discovery	Network Service Scanning	Software Deployment Tools	Data from Local System	Fallback Channels	Exfiltration Over Physical Medium (1)	Firmware Corruption
Spearphishing via Service	System Services (2)	Create Account (3)	Event Triggered Execution (15)	File and Directory Permissions Modification (2)	Network Sniffing	Network Sniffing	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Inhibit System Recovery
Replication Through Removable Media	User Execution (2)	Create or Modify System Process (4)	Exploitation for Privilege Escalation	Group Policy Modification	OS Credential Dumping (8)	Password Policy Discovery	Use Alternate Authentication Material (4)	Data from Removable Media	Multi-Stage Channels	Exfiltration Over Web Service (2)	Network Denial of Service (2)
Supply Chain Compromise (3)	Windows Management Instrumentation	Event Triggered Execution (15)		Group Policy Modification	Hide Artifacts (6)	Steal Application Access Token		Peripheral Device Discovery	Permission Groups Discovery (3)		Data from Removable Media
Trusted Relationship			External Remote Services	Hijack Execution Flow (11)	Impair Defenses (6)	Steal or Forge Kerberos Tickets (3)	Process Discovery		Data Staged (2)	Non-Standard Port	Transfer Data to Cloud Account
	Hijack Execution Flow (11)		Process Injection (11)	Indicator Removal on Host (6)	Steal Web Session Cookie	Query Registry	Email Collection (3)		Protocol Tunneling	System Shutdown/Reboot	
Valid Accounts (4)		Implant Container Image	Scheduled Task/Job (5)	Indirect Command Execution	Two-Factor Authentication	Remote System Discovery		Input Capture (4)	Proxy (4)		
				Masquerading (6)		Software Discovery (1)		Man in the Browser	Remote Access Software		
								Man-in-the-Middle (1)			

12 Tactics, 290+ Techniques, & Sub-Techniques

# Comparing Threat Identification Methods

## Simple Threat Identification

- **Generic identification** of physical, environmental, & man-made threats
- **Generic categorization** of purposeful, unintentional, or environmental threat categories
- **Generic assessment** of threats & risks based upon potential impacts:
  - Modification of data
  - Data destruction
  - Unavailable accurate records
  - Denial of service
- **Compliance-oriented**

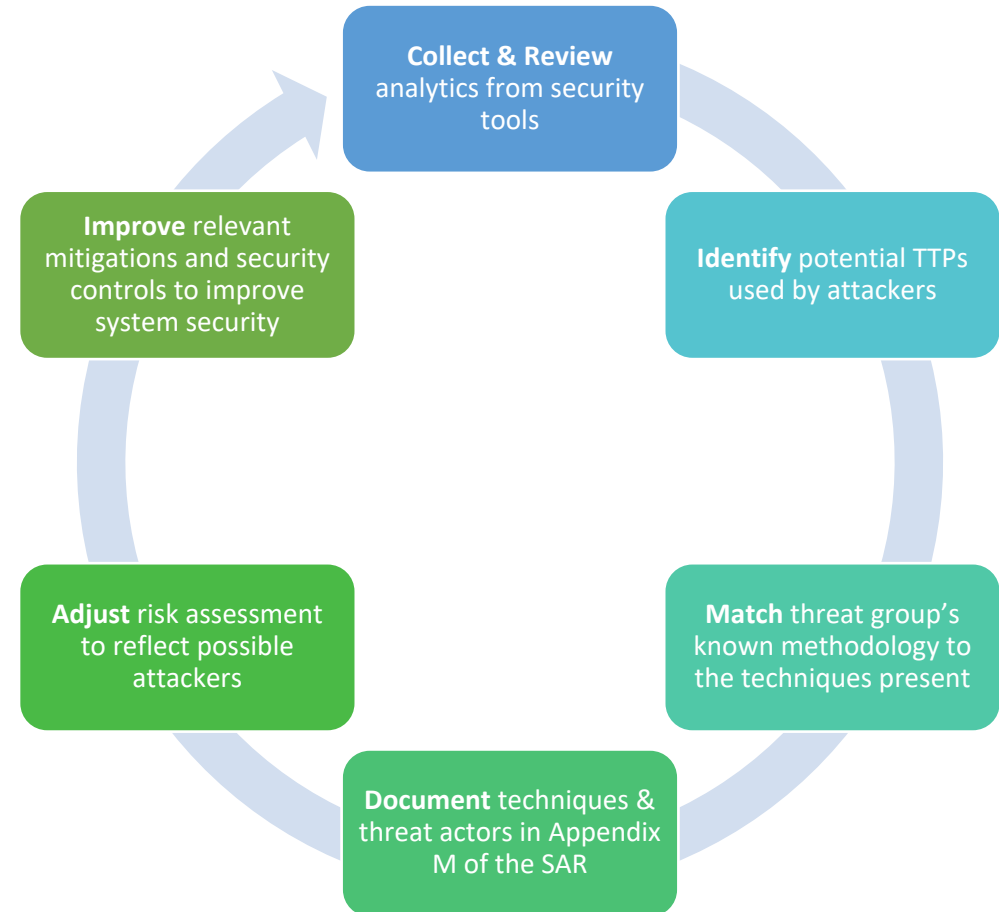


## MITRE ATT&CK Cyber Threat Identification

- **Identification of specific threat actors** based upon real-world observations of tactics, techniques, & procedures (TTPs)
- Used to understand the **process** of a cyber attack, instead the end result
- **Map** threat actor TTPs through different stages of cyber attacks
- **Threat-oriented**
- **Actionable**

# Using MITRE ATT&CK in Security Assessment Reports

- How can artifacts from penetration testing, vulnerability assessments, code reviews, tech support tickets, logs can be mapped to MITRE ATT&CK?
- How can these artifacts be mapped to MITRE ATT&CK tactics, techniques, and procedures (TTPs)?
- How can threats be identified using these TTPs?
- How does this change the assessment of risk to the system that was assessed?
- How can threats from these threat actors be identified and mitigated against?



# Using MITRE ATT&CK in the Cloud

## Analytics:

- Use security tools to create, collect, and analyze security analytics from sources such as AWS CloudTrail logs, Office365 audit logs, network device logs, and authentication logs
- Analytics can be collected using other methods such as monitoring processes on endpoints and how processes are using network resources

## Detection and Mitigation:

- Identify common vectors of attack or indicators of compromise (IOCs)
- Identify how to detect and mitigate against attacks

## Security Engineering:

- Identify gaps in security control coverage
- Make risk-informed decisions on security control deployment
- Improve efficiency of security control investments

## Penetration Testing:

- Take results of penetration testing and vulnerability assessments and map them to MITRE ATT&CK to identify how to detect and mitigate against attacks
- Emulate adversary behaviors during penetration testing

# Project Outcomes

## Lunch & Learn Presentation

- Introduced MITRE ATT&CK to over 150 NIH stakeholders and taught them how to use MITRE ATT&CK in Security Assessment Reports
- Opened dialogue between the A&A team and other teams such as Threat Management and Incident Response (TMIR) on using MITRE ATT&CK
- Opened the door for the use of MITRE ATT&CK across NIH

## Wiki Article

- Provides the first written internal resource that NIH Information Security stakeholders can reference on MITRE ATT&CK and its applications

## A&A Team Experience

- Very supportive staff and supervisors who mentored me throughout the fellowship
- Supervisors also helped me navigate bureaucracy and understand how bureaucracy could impact my projects
- Meetings with staff across NIH InfoSec including the CIO
- Amazing team dynamics! Staff was incredibly supportive and accessible.
- Inspired me to apply to the TechCongress Innovation Scholars Program